Pryvate

Communication Encrypted

Find answers to our commonly asked questions

FAQ

Table of Contents

General 1

WHAT IS PRYVATE?

Criptyque Limited offers The Pryvate™ App, an ever evolving Communications Security Solution that is delivered as a downloadable App for ease of use by our customers.

Once you are a part of the Pryvate™ Community you will benefit from real Communications Security. Initially across all your Voice calls, Conference calls, Video calls and IM along with any file transfers such as pictures etc.

These are our initial offerings with many more soon to be released to secure your email accounts and internet browsing

IS PRYVATE SECURE?

Yes. Pryvate™ uses Device-to-Device encryption technology, meaning only Pryvate™ app users exchange keys for each
peer-to-peer call. The keys are not held on a server. Pryvate™ uses the ZRTP protocol to encrypt the data packets of the
phone call across the Internet. Pryvate™ uses our secure Pryvate™ network servers to facilitate the calling service and
provide for complete security.
You can download the Pryvate™ white paper on ZRTP to understand the technology used for our encrypted voice, video
and conference calling.

CAN I USE PRYVATE ON MY DEVICE?

Currently if you have a device running iOS version 6.0 or Android version 2.2 then you can use Pryvate™. Other platforms will come online shortly. (Windows, Blackberry, Symbian etc.)

WHAT IS A MAN IN THE MIDDLE ATTACK (MiTM)?

A MiTM attack is when an attacker sits between two communicating end points, intercepting and forwarding data passed between the two as if he was not present. In doing so the attacker is able to eaves drop on communication between the two endpoints.
In the case of encrypted communications, the attacker will establish a secure connection with each end point acting as the other to each side. It is important to understand that two completely different encrypted communication legs are established during this attack. Both sides believe they have negotiated encrypted communications with the other, when in fact they are negotiated to the attacker. The attacker decrypts received information by one side, eavesdrops, reencrypts the data, forwards it to the other side and the end points are none the wiser.
Pryvate™ uses a Short Authentication String (SAS) to verify and confirm encryption key integrity as well as the user on the other side. They are the 2 randomly generated words you see on your screen when you call another Pryvate™ subscriber for the first time.

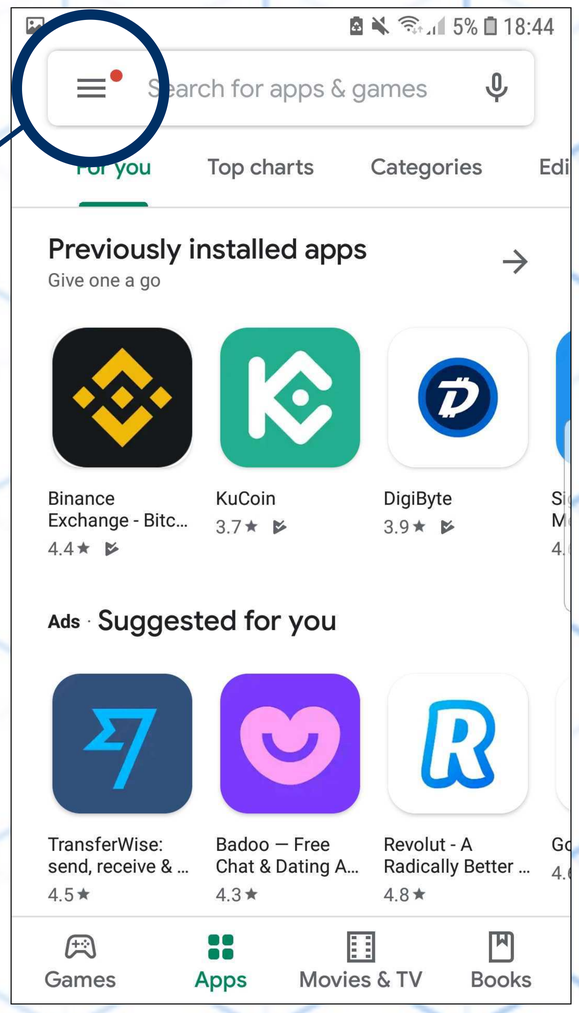
HOW DO I DOWNLOAD PRYVATE ONTO MY DEVICE?

Android
If your device is running Android 2.2 or higher then go into Google Play and search for Pryvate™ app. If not obvious then search for Criptyque. Download and then use the get started button on the www.pryvatenow.com main page.

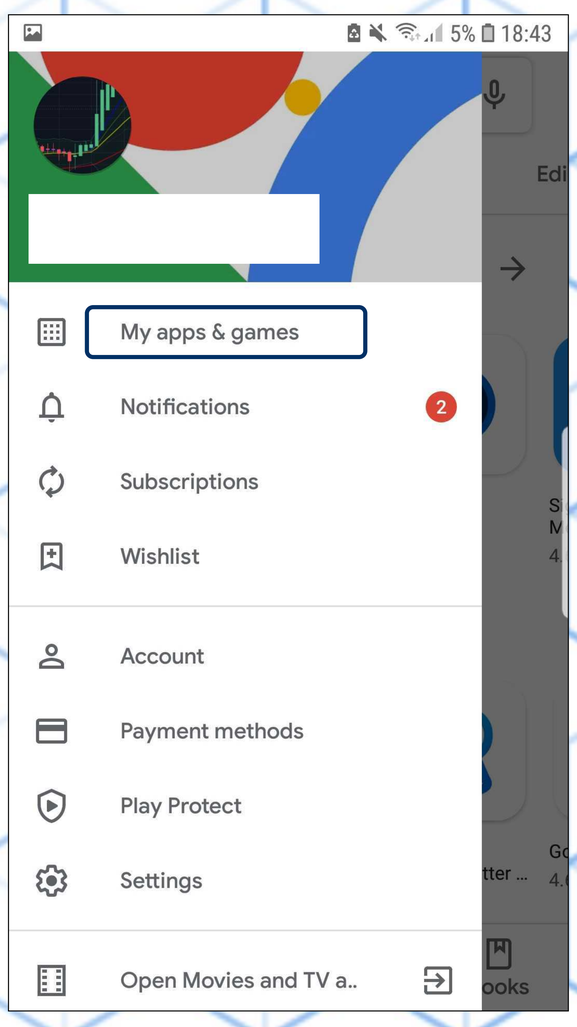
Apple IOS 6.0 or later
Search for Pryvate™ in the Apps store and download. Use the get started button as above.

HOW DO I UNINSTALL AND REINSTALL PRYVATE?

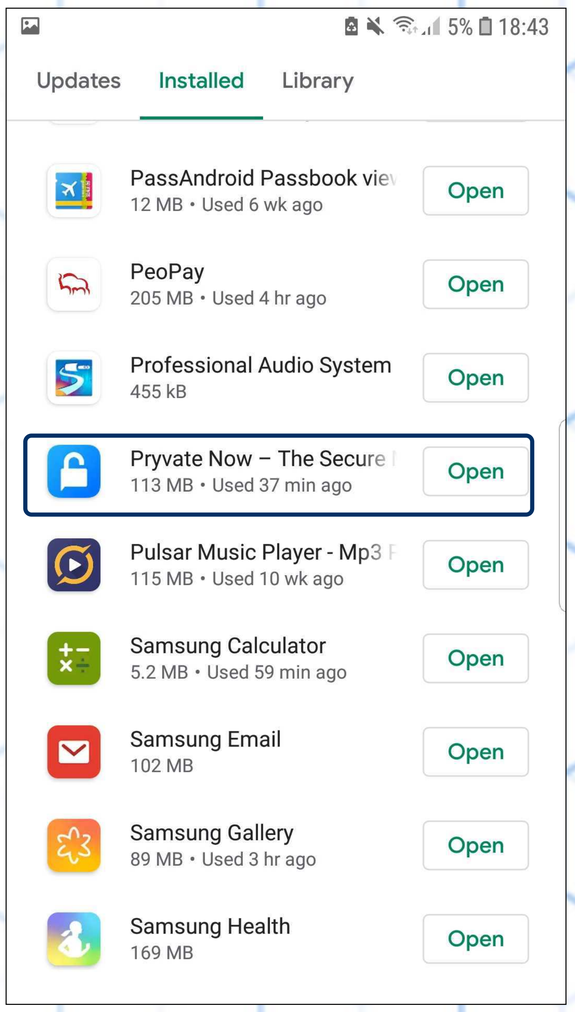
On Android you need to use Play Store. Open Play store and you will see the main Apps screen.



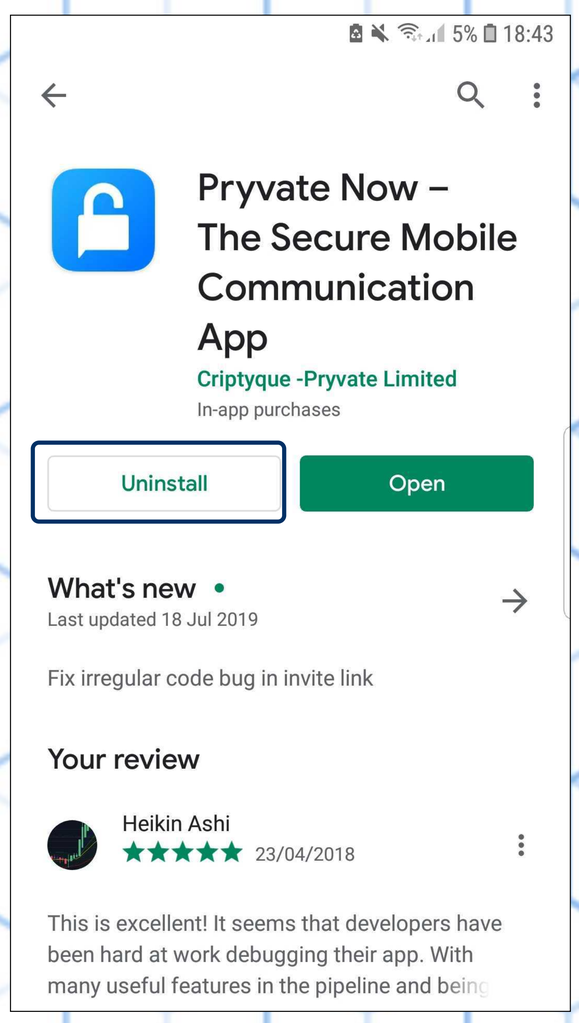
Click the three lines top left and you will see your options screen. Select My Apps.



Scroll down until you see Pryvate. Select pryvate and you will see two options. One is to uninstall.



Select uninstall and Pryvate is gone. To reinstall download it from Play Store and use your original installation instructions.



WHAT DEVICES DOES PRYVATE CURRENTLY SUPPORT?

IOS devices – Requires iOS 6.0 or later. Compatible with iPhone, iPad, and iPod touch. This app is optimized for iPhone 5.
Android – Any Android device running Android 2.2 or later. Smartphones and tablets.

DOES PRYVATE SUPPORT BLUETOOTH?

Yes. Your device will work as normal.

HOW BLUETOOTH HACKING WORKS

Bluetooth hackers set up specialized hardware and software that searches for vulnerable devices with an active Bluetooth connection. This usually happens in busy areas where commuters or consumers congregate. Your device, if hacked, will give no warning or indication that someone has accessed the information. All hacking must take place within 10 meters of the device being hacked; once the device is out of range, the connection is lost.

TYPES OF BLUETOOTH HACKING

Bluetooth hacking comes in two major varieties: 'Blue-snarfing' and 'Blue-bugging'. Blue-snarfing is when hackers connect to your device via Bluetooth and access the information on it. Many hackers quickly download the data so that they still have it, even if the device goes out of range. Blue-bugging allows hackers to make calls, send text messages and access the Internet via the connection, in addition to accessing the personal information on your phone.

DANGERS OF BLUETOOTH HACKING

Bluetooth hackers can use your phone's Bluetooth connection to make phone-based payments or call pay-per-minute numbers. These charges appear on your phone bill at the end of the month. Even if the phone is not used to steal your money, hackers can download your texts, photos and other vital files. This identifying information can be used as blackmail or for identity theft.

PROTECTING YOUR PHONE

The best protection against Bluetooth hacking is to turn off Bluetooth when you are not using it, especially in busy areas where hackers may search for devices. If you must leave Bluetooth on, make sure that the device is not set as discoverable; many phones only allow the device to be discoverable for a brief period of time. Do not initiate new pairing requests in busy areas. Never accept pairing requests that come up at random.

CAN YOU MAKE EMERGENCY CALLS WITH PRYVATE?

NO. You would use your phone as normal for this as the mobile phone is designed to utilise the strongest available network to connect irrespective of the carrier you are subscribed to.

HOW CAN I BE SURE THAT THERE IS NO ‘BACK-DOOR’ACCESS?

To the microphone or cameras that can side-step your encrypted applications?
You cannot. Spyware is the only way to defeat this level of encryption. Most spyware is exactly that. Written to be undetectable. The best way to avoid spyware is not to install any ‘Free’ games or apps. Keep your phone pure to avoid spyware

DOES PRYVATE WORK ON 3G/4G OR WI-FI? WHICH IS BETTER?

The quality of the voice or video will not be affected by the levels of bandwidth used on 3G, 4G or Wi-Fi. If you suspect that you have low bandwidth you can always run a speed test to see which gives you the better bandwidth. We like to use ‘Speedtest’. (www.speedtest.net) One point to note; When travelling roaming charges will apply to mobile data.

ARE MY COMMUNICATIONS COMPROMISED IF I USE A WIRELESS BLUETOOTH HEADSET?

Yes, is the short answer. To understand the answer, you must understand Bluetooth hacking. Then you choose whether or not to use Bluetooth or when and when not to use it. Note. If you are being specifically targeted, then the attacker has to be within 10 meters of you. Bear this in mind when driving.

CAN PRYVATE BE USED ABROAD?

Yes. As long as you have an internet connection you can use Pryvate™ as normal. Whilst there are no charges for using Pryvate™ you may encounter roaming charges from your service provider if using 3G or 4G. Pryvate™ can even be used in countries with deep packet inspection servers. (Those that block certain apps from Internet connection).

HOW DO I MUTE THE MICROPHONE DURING A VIDEO CALL?

As per a voice call.

HOW DO I MUTE THE MICROPHONE DURING A VIDEO CALL?

As per a voice call.

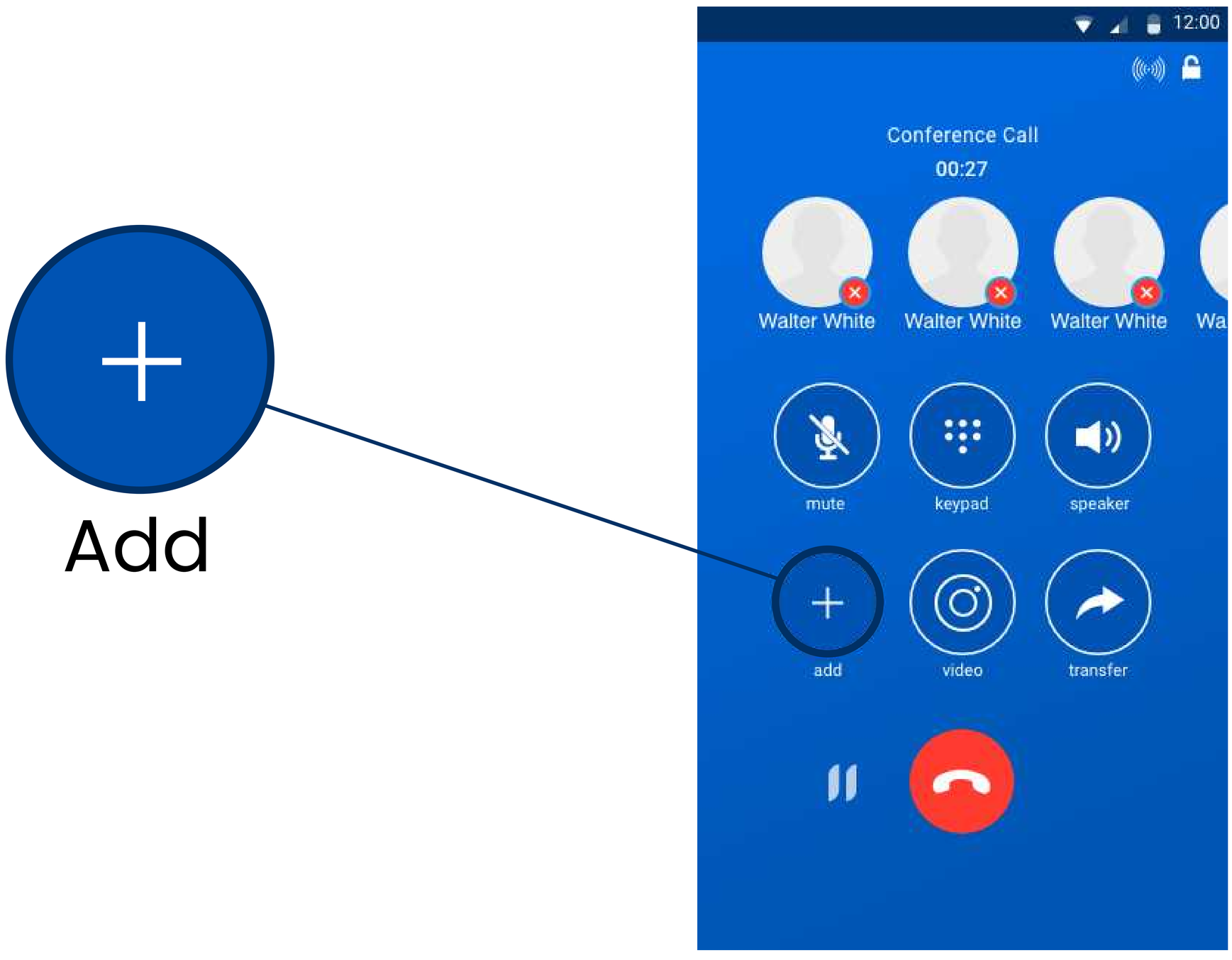
HOW DO I SWITCH BETWEEN CAMERAS DURING A VIDEO CALL?

You cannot. The cameras are fixed in the application.

Secure Conference Calling Service 13

HOW DO I INITIATE A CONFERENCE CALL?

Once you initiate a normal voice call you can then initiate a conference call. When the call is active look at the bottom left and see the Add button..This allows you to add a caller or transfer the caller to another Pryvate connection.

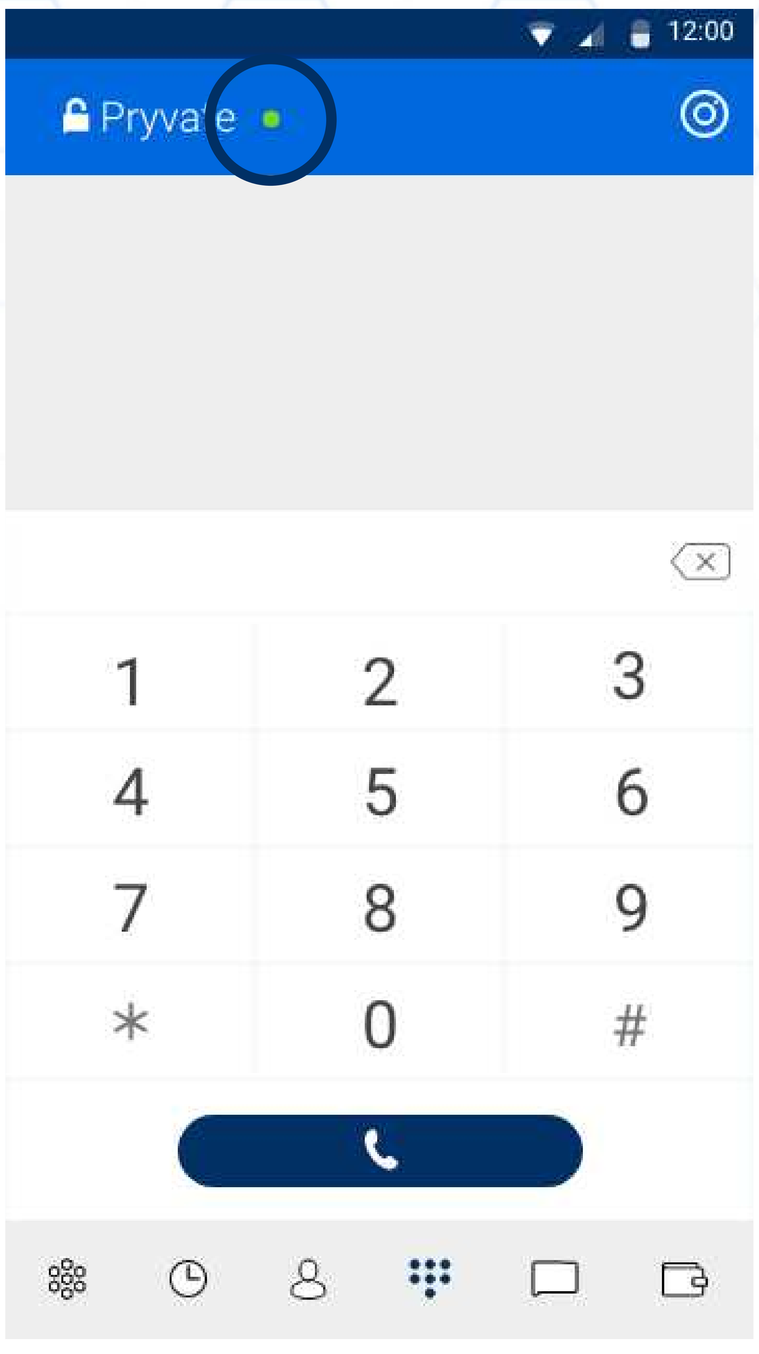


HOW DO I PUT A VOICE CALL ON HOLD?

On the bottom of the screen you will see a pause icon Simply press it. The person on the other end will hear music. The Pause will change to a play icon. To take the caller off hold simply press the play icon.

Secure Voice Service 8

HOW DO I MAKE A PHONE CALL?

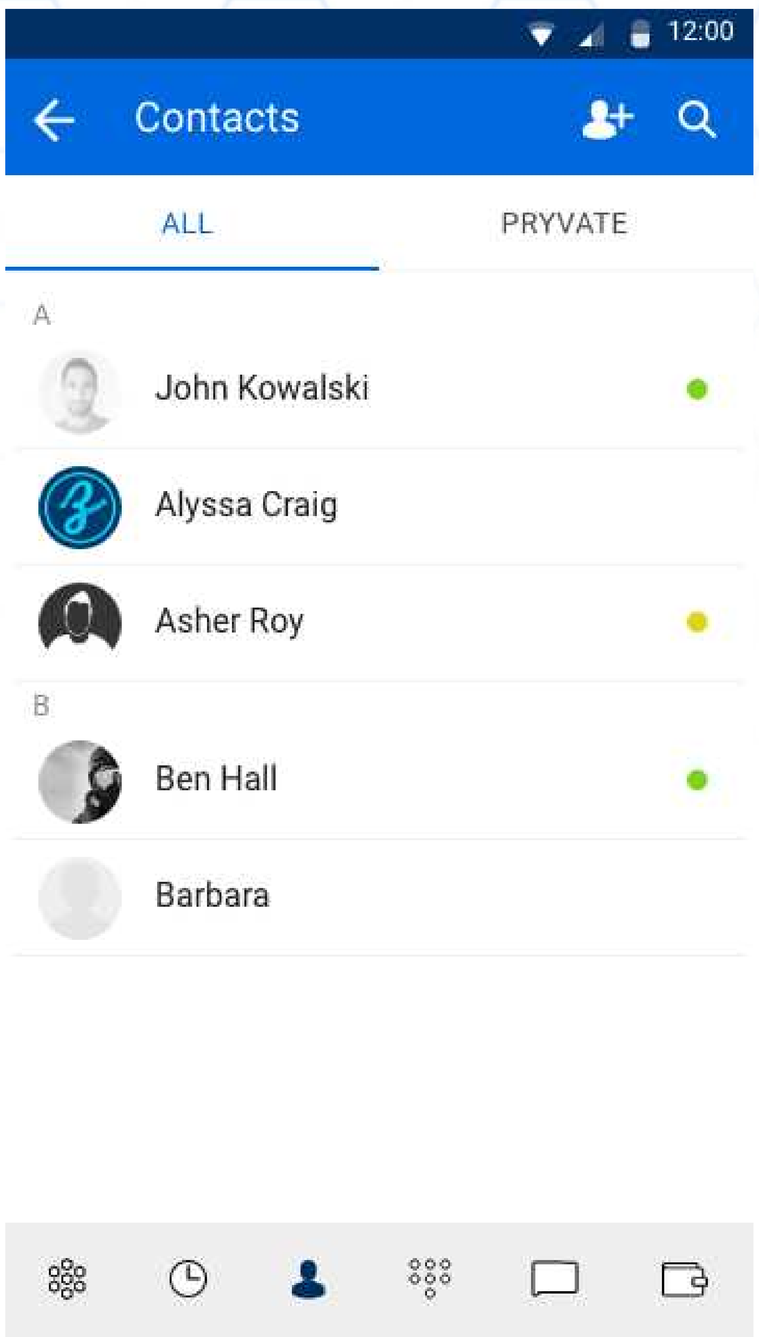


Once your service is active you will see a green dot at the top of your device and also you can open your app.

Once you open the app you will see the operator screen. Press Telephone symbol to open main dialler screen.If you know

If you know the Pryvate subscriber's number to be dialled then simply dial it and click the telephone button to make the call. Simply dial as an international entry. For example, in the UK it is +447888 123456 and the US it would be +1XXXXX XXXXXX etc.

Secure Voice Service 9



If it is to a former trusted Pryvate number and it is in your contacts, then select the contact and press the call button. Note that your normal number is secured through the app. Your normal number is your secure number. You just need to let users know you are Pryvate.

HOW DO I BRING UP THE KEYPAD DURING A CALL?

Activate bottom menu as per your devices instructions. Example on an Android HTC ONE M8 press the bottom of the screen and swipe upwards. Select as required.

CAN I DIAL NON-SUBSCRIBER NUMBERS?

No. The Pryvacy app is peer to peer only.

DOES PRYVATE™ HAVE VOICEMAIL?

NO. Voicemail is a security weakness of any communications system. However, the app will register missed calls in the
call history.

HOW DO I MUTE THE AUDIO DURING A CALL?

Simply press the microphone icon to Mute/Unmute

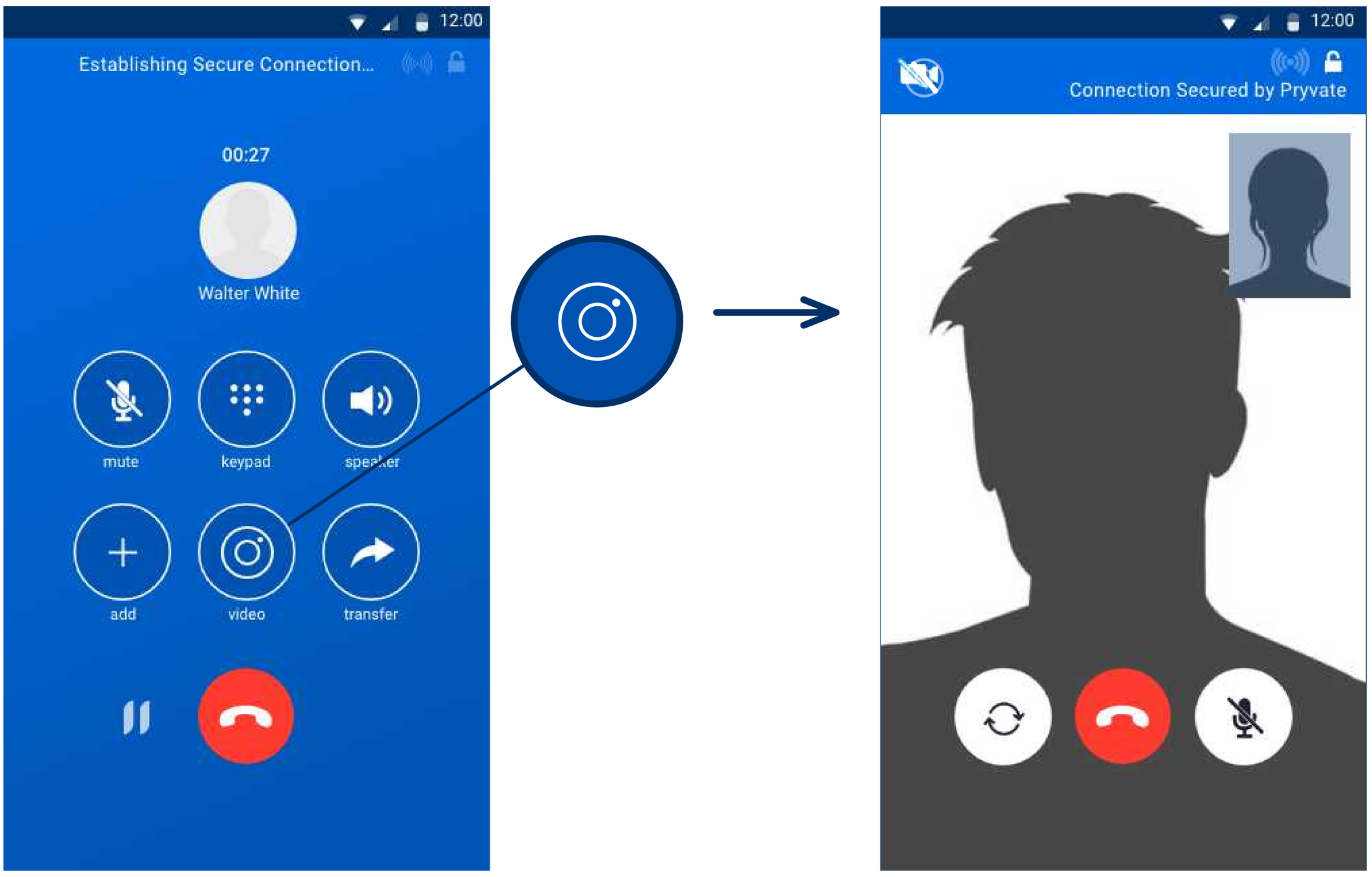
Secure Video Service 11

HOW GOOD IS THE VIDEO QUALITY?

As you are not competing with anyone for contention you will find the video quality of Pryvate™ as good as a television
picture. Its real time with virtually no lag unlike Skype who has many users going through the same server. Your secure
video is peer to peer.

HOW DO I INITIATE A VIDEO CALL?

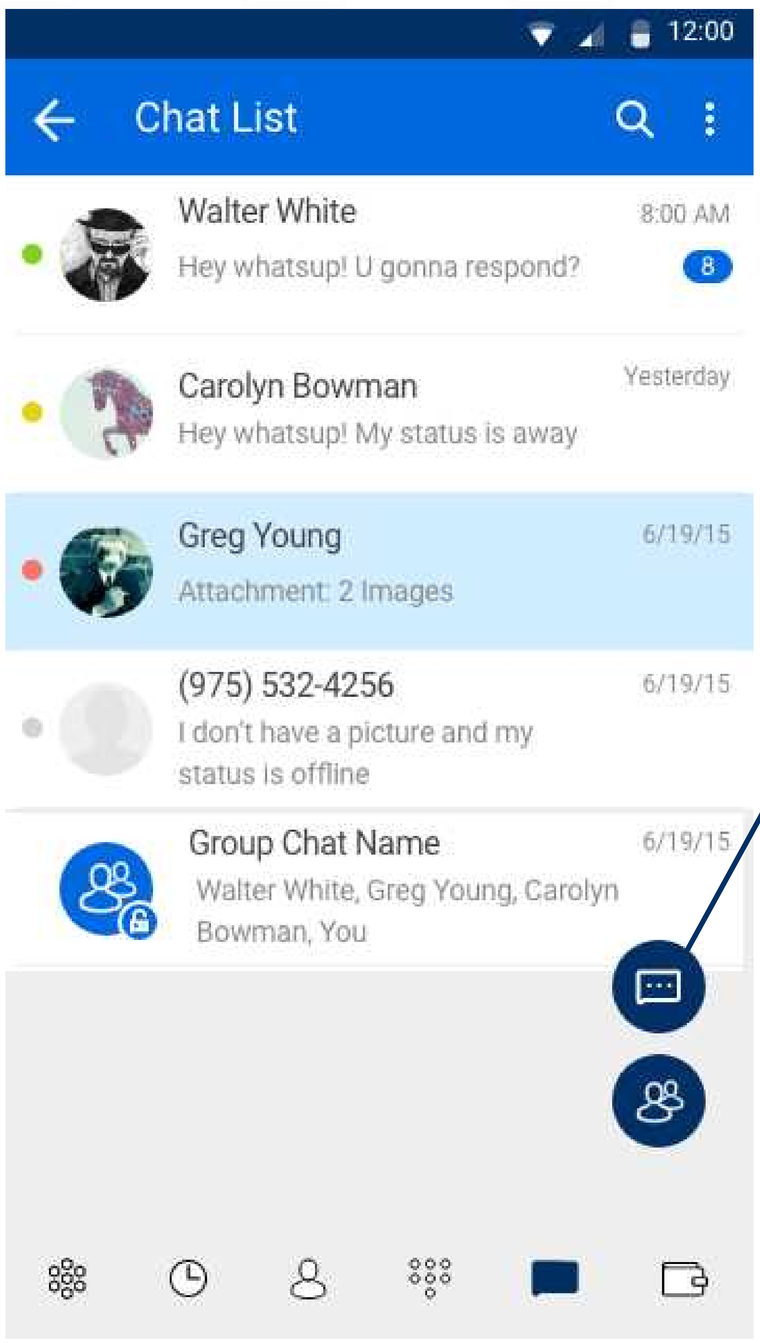
One a voice call is initiated you can then switch to video by pressing the video button. The switch is immediate

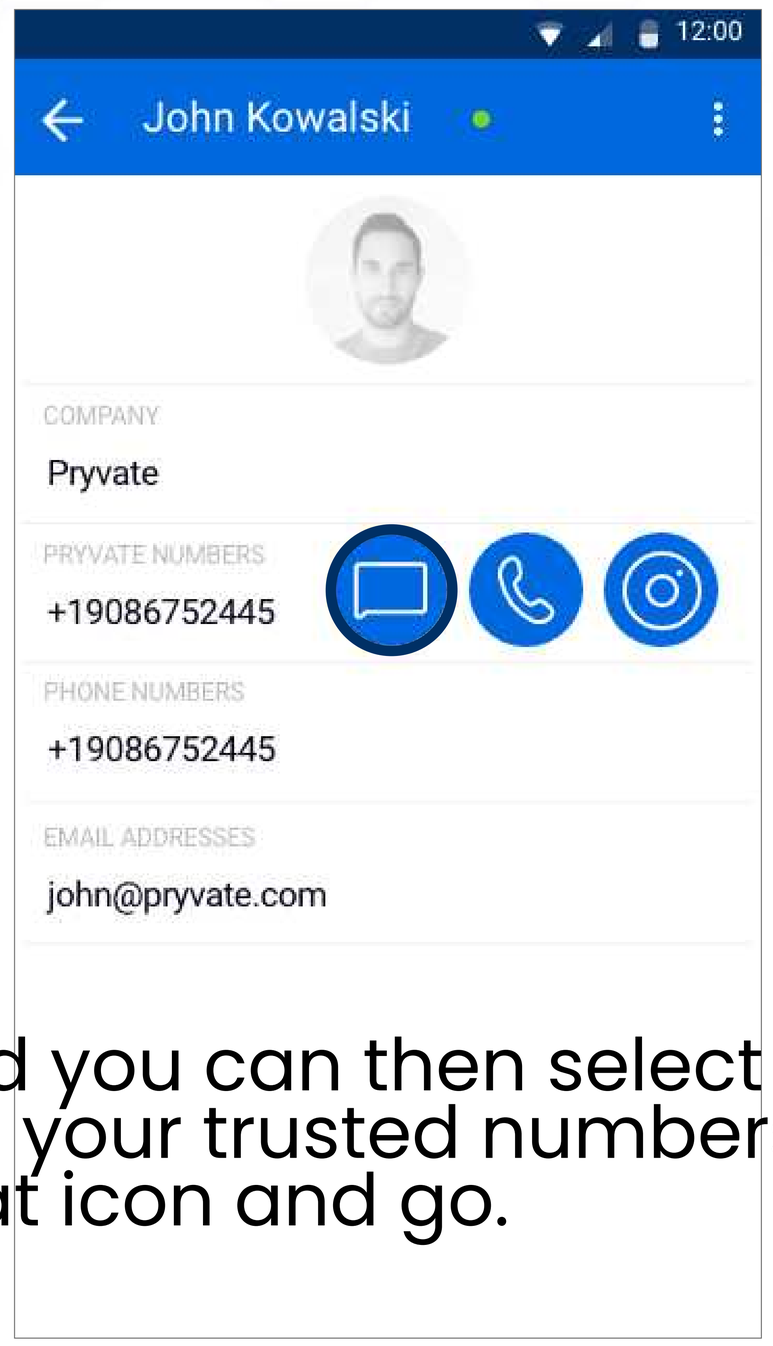


HOW DO I INITIATE SECURE IM?

Before you can securely IM someone you need a trusted relationship with that persons' number. To do this simply make a call as normal. Once trusted you can IM as and when you wish. They can receive and send if they are connected to the internet. No different to using SMS on a mobile phone. Once the mobile number is trusted then simply follow the following instructions:

Open the app and select the chat Icon



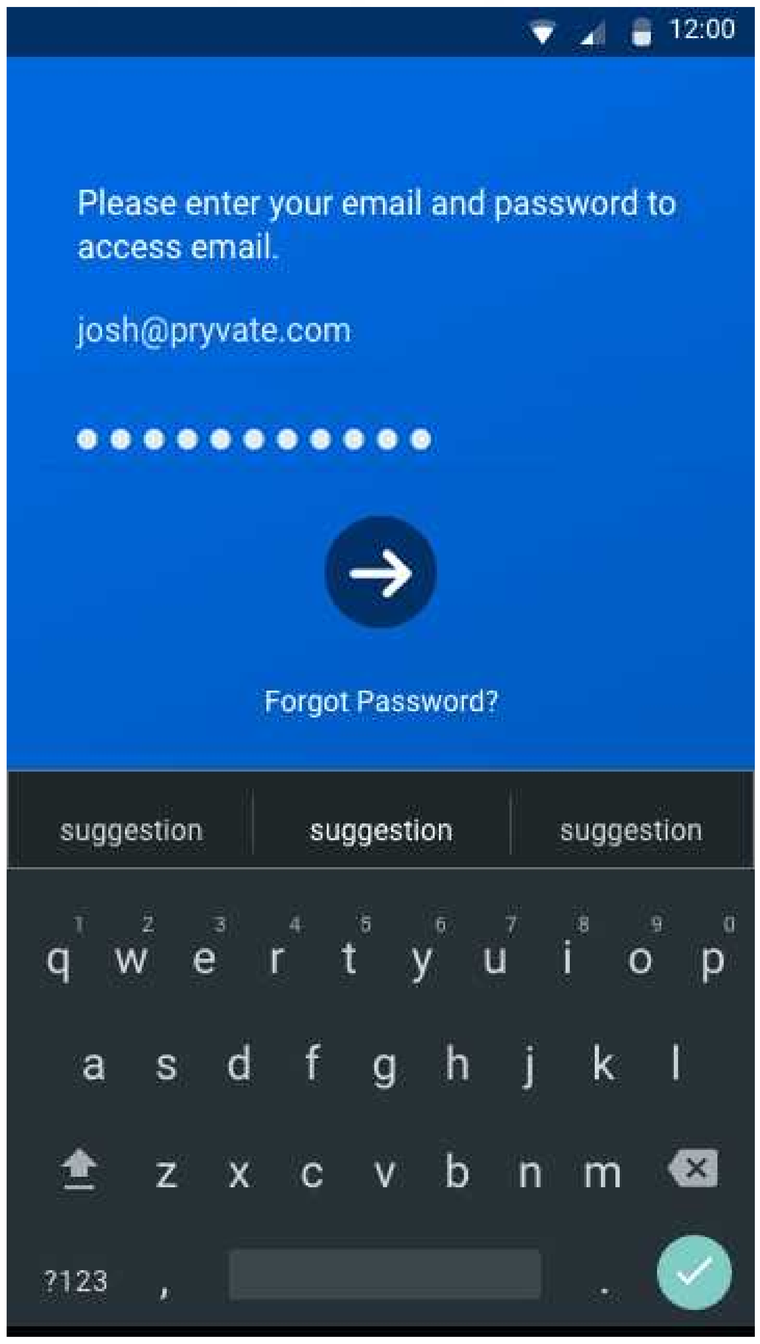


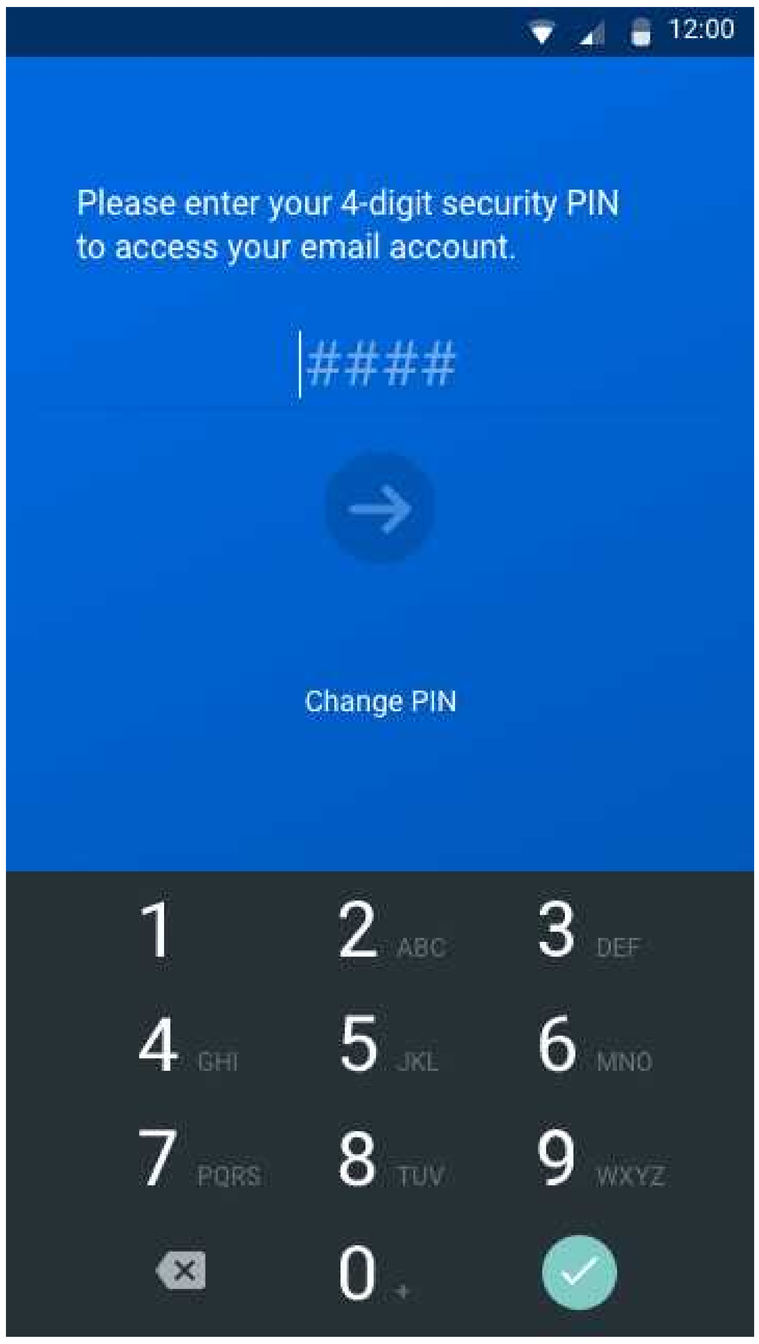
Once pressed you can then select your contact from your trusted numbers. Press the chat icon and go.

Then message as you would do with any other IM application. You then see the contact selected.

HOW DO I ACCESS MY SECURE EMAIL?

When you open your Pryvate app, the ‘EMAIL’ button will be the bottom left button on the home screen. Press this to open the secure email screen. Enter email address you registered with along with password. Your password would have been mailed to your Registered Email Address. If you forgot your password click “Forgot Password” to recover. You will then be prompted for your 4-digit Security PIN.





HOW DO I SEND A SECURE EMAIL?

You first need to login with the email address you registered at secure email signup. Then you login, and send the email as a normal mail. The app will take care of the security and encryption of your messages

WHAT IF THE PERSON I AM EMAILING IS NOT ON PRYVATE™ SECURE EMAIL SERVICE?

Unfortunately, you will not be able to send a secure email to a recipient who is not on the Pryvate™ secure email service. When you attempt to do, you will get a prompt to say “Recipient is unregistered, do you want to send message as plain text?” and you can then send the email as a regular unencrypted email.

WHY ARE MY SECURE EMAILS COMPOSED IN THE APP, BUT GET SENT OUT USING MY REGULAR EMAIL CLIENT? IS THIS SECURE?

Yes. The email is sent via your regular email service so you do not have to change your current email address. However, the email sits in your regular email service, but in encrypted format and can only be read when open on your device since only your device has the private security keys to decrypt the message. Hence your email is still secure.

Presence

Automatic discovery of your contacts that are on Pryvate app, auto notification when contacts become a Pryvate user, auto population of Pryvate address book, Enables Pryvate users to see when their connected contacts are available for a fully secure call or video call.

Self-destruct on IM

Ensures the content of an IM chat can be securely deleted from both users' devices and is irretrievable by anyone.

Notifications on screenshots

Detects when a screenshot is taken in the Pryvate™ app, and warns the sender that their recipient is attempting to photograph their confidential information. This can also indicate that the recipient's mobile device has been stolen or is being used for criminal content or simply that recipient wishes to keep a copy of the Chat.

Agnostic secure email

Enables secure email to be sent from any platform to any platform, such as Android to iOS and vice versa, and on any email client of the user's choice. This ensures users do not need to be retrained on new platforms and IT staff can keep their existing procedures in place without having to back up.

It's No Secret, We Deserve PRIVACY!

Pryvate

Powered by Criptyque